



eEye Digital Security®

**Blink: Protection from the
Threats of Today and Tomorrow**





Blink: Protection from the Threats of Today and Tomorrow

Introduction

A war is being waged against the desktop. Attacks against desktops within home and business networks occur every day, all in an attempt to gain unrestricted access to these systems. Attackers are smarter and more potent than they were in the past, many times being driven by stated intentions or monetary gain. Regardless of an attacker's intention, the exploit process, whether for intrusions or scams, follows a common script. Fortunately, we at eEye Digital Security know that script by heart.



eEye Digital Security has been at the forefront of learning how attackers exploit systems for over 10 years. While trends in attack scenarios has been moving rapidly over the past few years, eEye has been able to leverage its intimate knowledge of vulnerabilities and exploits to develop Blink[®], the most advanced host-based protection suite on the market. The result is best-in-class protection for every desktop, as well as ease of mind for IT security professionals.

Mass Exploitation vs. Targeted Attacks

Mass exploitation incidents (such as the notorious Italian Job MPack release) are widespread, effective and troubling. Such incidents can result in a large botnet being formed within only a few hours, becoming a very powerful attack tool used by the perpetrators for later malicious activities. Furthermore, the speed at which these incidents occurs is so rapid that, by the time it is reported publicly, the mass infection has already achieved the malicious goal of the attacker.

Perhaps more important is the type of attack that doesn't gain public notoriety for a number of reasons: targeted attacks. In these scenarios, an attacker has a specific goal within an organization or individual. Depending on the value of the target, many times an attacker will employ zero-day exploits as well as custom malware that bypass AV signatures. Both scenarios are very serious for any organization, but the one that ends up with the most serious impact will tend to be the targeted attack, as this is when intellectual property and data are at the most risk.

While most businesses are able to react to mass exploitation scenarios, nearly none are able to quickly react to a targeted attack. Worse, many attacks achieve their goal and disappear before anyone in the target network has even noticed the malicious activity.

The Move to Client-Side Attacks

Hackers are moving from network-based attacks to client attacks. Recent trends show that client-side applications pose the greatest risks today. Unfortunately, the large NIDS/NIPS market that so many organizations rely on is rendered useless against most client-side exploitation attempts, which operate below their radar. Whereas most network-based protocols are simple and commonly documented in RFCs or knowledge bases, client-side file-formats are rarely documented and are incredibly convoluted.

The other main threat facing the desktop is browser-based vulnerabilities. Browser-based vulnerabilities are very simple to exploit since user-interaction is typically easy to influence. Under some circumstances, even a visit to a trusted site could be dangerous. Even though this traffic is being sent across the well-documented HTTP-protocol, it can be obfuscated by the attacker to render any in-line network-based IPS system useless against the traffic since the NIPS does not have the functionality capabilities of the end-user's web browser (i.e. JavaScript / VBScript).



Unfortunately, file-format and browser-based vulnerabilities represent a majority of the exploits being launched in successful real-world attack scenarios today.

Generic Memory-Based Protection is Essential

When unknown zero-day exploits are unleashed against a system, the only defense that users have is generic protection from their host-based security solution. eEye has developed Blink's System Protection functionality. A portion of this functionality is the monitoring for potentially malicious activity within a process and protecting the system from exploit code by terminating and restarting the process prior to exploitation. There is literally no other way to protect systems from the unknown. While Blink is not the only host-based tool to protect in this manner, "Blink can provide a superb breadth of power in a single well-designed and solid package."- VB100. In simple terms, Blink has successfully blocked every identified memory-based user-land exploit since its inception; a track record that should resonate with those who have been impacted by unknown exploits.

This gives IT administrators the advantage to roll out mitigation or patches on their own time with peace-of-mind knowing that their systems will be protected.

Generic Anti-Virus Protection Must Be Implemented

Many AV vendors rely specifically on collecting malicious binaries in the wild and writing signatures for those samples. Unfortunately, this does not proactively prevent unknown malware from infecting users before the AV company has been able to attain a sample. Because of this specific reason, Blink has multiple layers of generic detection methods above the malware signature engine. These mechanisms include several heuristic modules, as well as a distinguishing utility known as a sandbox. Within this sandbox, a binary is run in a full Windows emulated environment to detect the full behavior of the binary prior to it executing on the host operating system. This allows for a very unique perspective on the functionality of a binary without previous knowledge of the sample, allowing for a very powerful extra-layer of defense for malware.

In simple terms, Blink has successfully blocked every identified memory-based user-land exploit since its inception, a track record that should resonate with those who have been impacted by unknown exploits.

To learn more, please visit www.eeye.com
or call 866.282.8276



Administrators Need to Know What's in their Networks



Although Blink does offer administrators the ability to avoid panic patching and patch their network when it's suitable for them, administrators still need to have a good understanding of what's on their network. eEye Retina[®] is the de facto standard for many organizations regarding vulnerability assessment, and this functionality has been embedded into Blink. Blink includes the lightweight Retina agent to scan itself on a continuous basis so that administrators can know exactly what vulnerabilities exist on their network and on which hosts. This becomes even more useful when vulnerability assessment scans are difficult because of a mobile workforce. The scans can be performed automatically and results are cached until connectivity to the internal network is regained in which they are uploaded to the REM management console.

A Security Vendor You Can Trust

Throughout eEye's 10-year tenure, we have been at the cutting edge of security research and development. While some security vendors may be staffed with non-security-educated developers, all of the engineers at eEye have an intense knowledge of all aspects of security. This enables our products to be more effective when protecting networks, while also avoiding any new vulnerabilities being introduced to an environment with a security solution, a very ironic but common occurrence. eEye has never had a vulnerability identified or exploited in any one of our products, and that tradition continues with Blink, the most secure and powerful host-based security solution on the market.

Readers of this document who wish for more detailed analysis into the underlying technologies of Blink and how Blink fights specific threats should review the full 'Deep-Dive' version of this document.

About eEye Digital Security

eEye[®] Digital Security is pioneering a new class of security products integrated threat management. This next-generation of security detects vulnerabilities and threats, prevents intrusions, protects all of an enterprise's key computing resources, from endpoints to network assets to web sites and web applications, all while providing a centralized point of security management and network visibility. eEye's research team is consistently the first to identify new threats in the wild, and our products leverage that research to deliver on the goal of making network security as easy to use and reliable as networking itself. Founded in 1998 and headquartered in Orange County, California, eEye Digital Security protects more than 9,000 corporate and government organizations worldwide, including half of the Fortune 100. **For more information, please visit www.eEye.com.**

While some security vendors may be staffed with non-security-educated developers, all of the engineers at eEye have an intense knowledge of all aspects of security.



eEye Digital Security[®]

To learn more, please visit www.eeye.com
or call 866.282.8276

